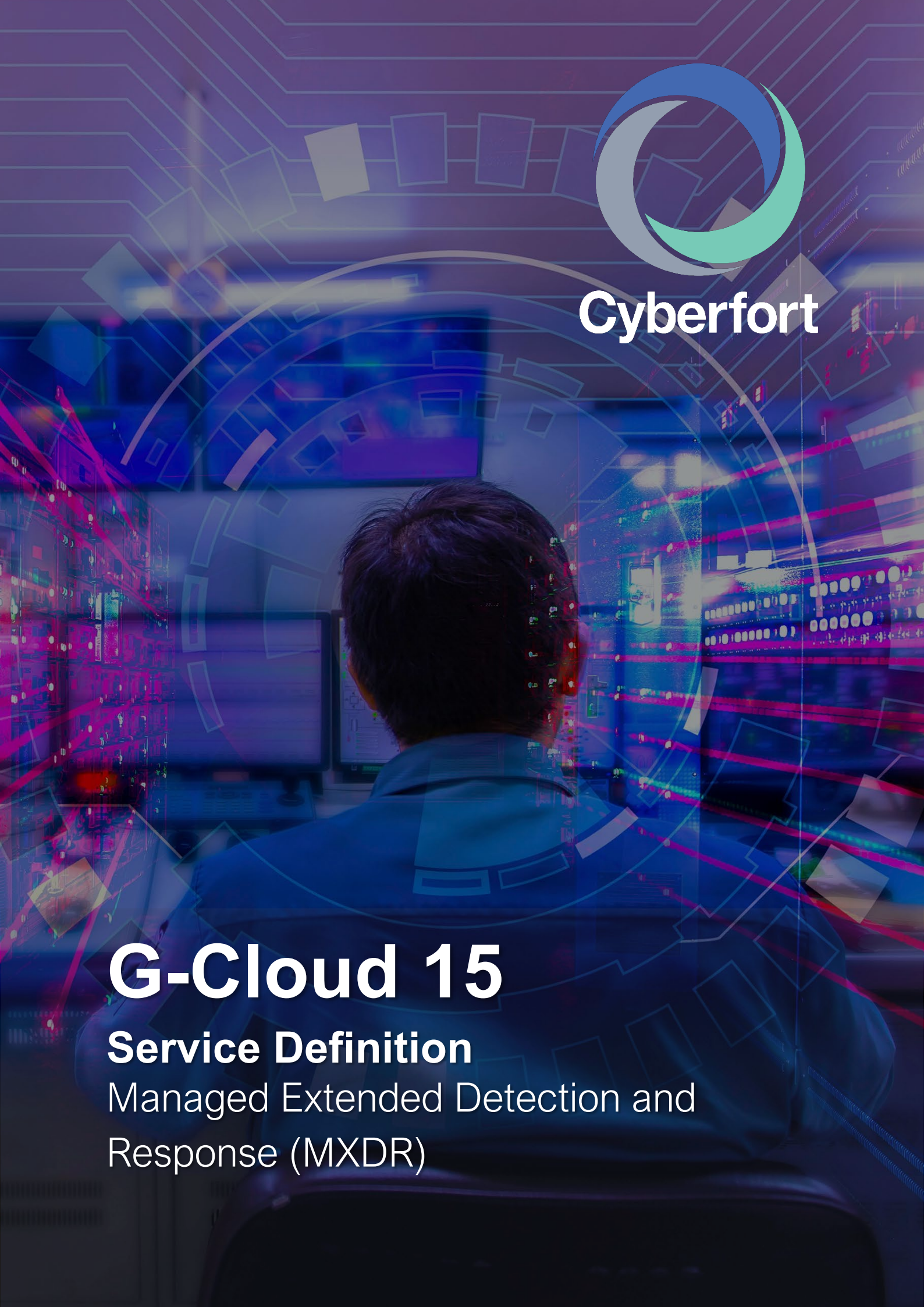


Cyberfort

G-Cloud 15

Service Definition

Managed Extended Detection and Response (MXDR)

Table of Contents

1. Service Overview

Cyberfort's Managed Extended Detection and Response (MXDR) Service delivers peace of mind by providing powerful insights into internal and external malicious activity, threats, and associated business risks; managed by our highly skilled Security Operations team using our Elastic Security SIEM platform, Elastic security Defender for EDR, Microsoft Sentinel and XDR, and other appropriate security technologies where required.

We'll deliver an innovative security service underpinned by cybersecurity best practices, delivered by our team of CREST certified analysts, using approved methodologies against standard frameworks, and integrating up to date threat intelligence and threat actor TTP's. Service management will work alongside our cybersecurity specialists, from day one you will have a combination of the best people and resources, using the best tools, delivering a best-in-class experience.

We pride ourselves on the ability to deliver a holistic approach by considering an organisation in its entirety, we will correlate the complexities of your environment delivering actionable advice and action to mitigate cybersecurity risks and improve the defensive posture of your organisations.

We will leverage your existing security tooling to gain visibility, context and an ability to respond – where you don't currently have an EDR solution in place, Cyberfort will deploy Elastic Security Defender EDR agent to endpoints at no additional licensing cost to provide enhanced endpoint defences, a further cost saving or both. Elastic Security Defender will result in some additional log storage costs but, in our experience, these will be comparable to existing endpoint protection tooling log costs.

Utilising the latest technology and industry best practices our service is provides enterprise level threat detection and response across your estate.

Cyberfort's Security Operations Centre comprises the following key elements:

- **Security Information and Event Management (SIEM):** Provide threat detection, compliance and security incident management through collection and analysis (both near real time and historical) of security events.
- **Threat Intelligence (TI):** Threat Intelligence is used to enrich event data providing context against current known threats to aid threat detection and event management.
- **Incident Management:** Security incident management to identify, record, analyse and manage security threats or incidents. Our team will manage these incidents to closure working with your teams to deliver peace of mind.
- **Continual Monitoring:** Continual monitoring of your estate with log and event collection and analysis to detect new indicators of compromise as they occur.
- **Use Cases:** Design, deliver and fine tune use cases to encapsulate detection and responses against specific threats.
- **Machine Learning (ML):** Machine learning enables threat analytics to automatically identify malicious activities.
- **Immediate Notifications:** We'll alert you as soon as an incident is detected and verified.
- **Peace of Mind:** We'll watch your estate while you run your business, allowing you to sleep soundly at night.
- **Experienced Analysts:** Our highly skilled analysts will investigate all alerts to reduce false positive alarms so you can focus on your job.

- **Storage Requirements:** Configurable rolling storage to meet client's needs, including compliance requirements.
- **Endpoint Detect and Response (EDR):** Next Generation EDR agents deployed on your assets to protect and monitor for malicious activity (if required)
- **Compliance Monitoring:** For compliance or regulatory requirement, where Security Monitoring is required, we are more than a tick box for you.
- **Management Reporting:** We will provide regular reports with key findings highlighting your cyber security posture.
- **Dashboards:** We will configure customised dashboards delivering a real-time view of vulnerabilities and threats.

1.1 Service Detail

1.1.1 Service Description

Cyberfort's Managed Extended Detection and Response 24x7x365 SOC service includes the following capabilities and services:

24x7x365 monitoring, detection, analytics and response defending your environment.

- Our MXDR provides continuous monitoring, detection, analysis and response, of the security posture of companies on an ongoing basis. We defend our clients systems, data, processes and people from cybersecurity incidents using a combination of technology solutions, security expertise and threat intelligence, underpinned by a robust set of independently accredited procedures.
- The Cyberfort SOC operates as your extended security team, defending your business 24x7 with security analysts and engineers. Our SOC staff work closely with clients during cybersecurity incidents to ensure issues are addressed quickly upon discovery.
- The SOC monitors and analyses activity on networks, servers, endpoints, databases, applications, websites, public and private clouds and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. It is responsible for ensuring that potential security incidents are correctly identified, analysed, defended, investigated, and reported.

Alignment to your organisation's risks, threat landscape and risk appetite

- Contextual awareness and prioritisation through threat modelling, enabling Cyberfort to understand your business and environment, how it is used, what the likely targets would be and how an attacker is most likely to gain access. This ensures that the security ROI is maximised, and by understanding your business, we are enabled to operate as an extension of your team.

Single Point of commercial and technical expertise

- Dedicated, named Commercial Account Manager who acts as your representative within Cyberfort, delivering a single point of communication, expertise and alignment for all non-technical matters, escalations and problem resolutions.
- Dedicated, named Technical Account Manager who acts as a first point of contact for operational matters and proactive management of high priority and ongoing incidents. As your technical friend within the service, the TAM will also provide maturity guidance and

recommendation on insights to improve your security posture discovered through monitoring insights.

Full incident profiling of alerts/incidents

- Our service is not based around alert passing, we utilise an approach of understanding what has happened, who/what it has happened to, the immediate recommended steps/actions to mitigate the risk, and recommendations for any changes or improvement to improve overall security and stop it happening again.

Active and passive responses to security incidents

- Active responses include containment and remediation (where available and appropriate) of devices, systems and identities and will utilise playbook and automation driven interactions with client's existing security tooling.
- Passive responses include guided recommendation on containment, remediation, and other changes to improve the strategic security of client's environment.
- Our offer includes full incident handling, there is no limit on incident handling, investigation and analysis/containment/incident support. Specific DFIR services are not included, the Cyberfort SOC will continue to work to support the incident, however, should specific DFIR capabilities be required, Cyberfort will work with your chosen DFIR partner. Effectively, The SOC team will provide ongoing and effectively unlimited Incident handling, however we are dedicated to continuous security monitoring, analytics and response rather than operationalised as a DFIR team.

Threat Hunting

- Our service includes scheduled and ad-hoc threat hunting for incidents in client data, driven by threat intelligence, incident hypothesis and using a trigger/investigate/iterate approach. Where appropriate client resources are welcome to participate in hunting if desired.

Threat Intelligence

- Our service includes the sourcing of threat intelligence from a number of open/closed sources, and we will provide threat intelligence briefing reports at a cadence to be agreed.

Detection engineering

- Our service includes detection engineering, including the generation of use cases, searches and queries to support detection of incidents and events within your environment.

Automation and playbooks

- Our service includes automation engineering and playbooks, following our normal process of undertaking a task 3x manually, we will look at ways to improve the automation flow for enrichment, detection, response and overall service efficiency.

Evidence and Reporting

- Our service includes monthly reporting to client, near real time data awareness with custom dashboards and workbooks to evidence the service value and effectiveness and enable visibility and awareness of the security posture, and a review of overall security posture at a cadence to be agreed, but at least annually.

Preferential rates for other Cyberfort service offerings

- Cyberfort will offer client a preferential rate on any other cyber security services requested, including pen testing, consultancy and compliance.

Continuous improvement & Efficiency

- Our service iterates and improves, continuing to tune and improve detections, analytics, response and automation to align with the evolving business, threat landscape and attacker techniques.

1.1.2 Monitoring

Our approach involves integrating with your existing security infrastructure to maximise the effectiveness of your service. We will collect and analyse the alerts generated by your EDR (Endpoint Detection and Response) from our own Elastic host agent solutions.

To ensure seamless integration, our team will work closely with your security teams to establish secure connections and configure the necessary settings. These connections can automatically retrieve the alerts generated by your security tooling, eliminating the need for manual intervention. This automated process ensures that all relevant alerts are captured in near real-time.

Once the alerts are received, our SIEM and analysts will apply advanced correlation and analysis techniques to identify patterns, anomalies, and potential threats. By consolidating and correlating alerts from multiple sources, our analysts have a holistic view of your organisation's security posture, enabling them to quickly identify and respond to potential threats.

In addition to collecting alerts, our service will also collect and analyse additional data from your ingested security tooling. This includes information such as device health status, malware detections, and system logs. By correlating and enriching this information, our analysts will deliver comprehensive insights into your organisation's security landscape, helping you identify vulnerabilities, track trends, and make informed decisions to enhance your security posture.

Our analysts utilise the power of our SIEM through customisable rules and policies, enabling specific actions and responses based on the severity and type of alerts generated. This enables us to automate incident response processes where appropriate under your governance, escalate critical alerts to the appropriate teams, and take proactive measures.

1.1.3 Threat Hunting

Included in our service is proactive threat hunting which searches across your infrastructure and endpoints to identify threats that may have evaded the security controls that are in place. We use a combination of machine assisted and manual techniques where expert led threat hunters search for indicators of compromise (IOCs) across your IT environment.

Our proactive threat hunting tactics have evolved to use new threat intelligence on previously collected data sources to identify potential threats in advance of any potential attack. By conducting regular threat hunting activities for evidence of a breach, our security teams are able to identify unknown threats and respond quickly and effectively before they cause damage and disruption.

Our experienced team of Blue and Red Team consultants have a deep knowledge and expertise of offensive security. They use and apply this knowledge to help identify unknown threats. This is enhanced by our actionable threat intelligence, ranging from IOCs and detection capabilities to strategic reports on tomorrow’s threat landscape.

We use an in-house developed threat hunting methodology to ensure that analysts are equipped with the latest tactics, techniques, and procedures to enable effective threat hunting campaigns.

Tried and tested methodology ensures a consistent approach and enables the SOC to concentrate on finding Tactics, Techniques and Procedures (TTPs) regardless of vendor diversity and difference in available datasets across client platforms.

Cyberfort utilise two forms of threat hunt:

Manual Hunts

These hunts are designed to be a manual investigation into the unusual behaviours within an environment, while they can have specific aims i.e. from threat intelligence however can also be used to assess “types” of behaviour such as user activity or network connectivity.

Manual threat hunting is normally conducted monthly, on each endpoint, relevant servers, and network devices. Should any suspicious activity be detected, the SOC will log an incident and follow the Triage, Investigation and Analysis process. Any other findings will be documented for the monthly service report.

Manual Hunts will typically run for approximately 3 hours with a detailed analysis of all findings and concerns being utilised to create new use cases, aid detections, and identify incidents.

Automated Hunts

Automated hunts are often used to assess volumetric data that allows us to search for high volumes of data in an automated and scheduled way. These will correlate data across the estate to ensure a broad assessment of security concerns.

Additional Ad-Hoc threat hunting exercises are typically performed:

- When there is intelligence regarding a breach or adversarial activity against a particular vertical industry or a vendor.
- Where specific intelligence regarding a new threat warrants immediate hunting for presence or indication of that threat.
- Under bespoke conditions agreed with you.
- As part of the playbook defined response or investigation of certain “use cases”.
- An adversary is looking for a specific port or vulnerability to compromise an internet facing asset.

1.1.4 Integrations and Ingestion Pipelines

Our engineering team will leverage a wide range of out-of-the-box APIs (Application Programming Interfaces) and integrations to ingest your data seamlessly and efficiently from your existing applications. These are designed to facilitate the seamless transfer of data between different software systems, ensuring that the information from your applications can be easily accessed and utilised within our platform.

Where the required APIs and integrations do not already exist, our dedicated team of experts will work closely with your organisation to develop custom APIs and integrations. This process involves thorough analysis and understanding of your applications' data structures, business logic and security requirements.

Developing custom APIs and integrations requires a high level of technical expertise and meticulous attention to detail. Our team will ensure that the APIs and integrations are robust, reliable, and secure, adhering to industry best practices and standards. We will conduct rigorous testing and validation processes to ensure that the data ingestion process is smooth, accurate, and efficient. We will provide ongoing support and maintenance for the APIs and integrations, ensuring that they remain up-to-date and compatible with any changes or updates to your applications. We understand that technology landscapes are constantly evolving, and our team is committed to ensuring that your data ingestion processes remain seamless and uninterrupted.

The Cyberfort engineering team will work in collaboration with client to ensure that the data sources along with telemetry from syslog, log files and NetFlow data from your operating systems, firewalls,

switches and routers, malware/antivirus software, ERP applications and VPN's is cleansed and sending through only relevant data into the SIEM.

1.1.5 MITRE ATT&CK Framework

Cyberfort analysts ensure effective monitoring, detection and response to cyber threats that are aligned to the MITRE ATT&CK framework. We leverage prebuilt security analytic content that includes detection rules aligned with MITRE ATT&CK framework. Our analysts can gain visibility into potential threats and help improve your overall security posture. Our engineering team refine and customise the alerts generated by the system based on their specific requirements and organisational context. By tailoring the alerts, security teams can focus on the most relevant and critical threats aligned with the MITRE ATT&CK framework.

1.1.6 Malware Intelligence Sharing Platform (MISP) and Security Orchestration and Automation Response (SOAR)

With every alert generated, the SIEM leverages the power of our MISP (threat intelligence sharing platform) and the automation capabilities of our SOAR (Security Orchestration, Automation, and Response) tool. This combination of resources enhances the analysis process for our analysts. The MISP platform plays a crucial role in enriching the alerts by providing access to a wealth of threat intelligence data. This data includes information from various sources such as open-source feeds, commercial feeds, and internal intelligence. By incorporating this additional context into the alerts, analysts gain a deeper understanding of the potential threats with which they are dealing. They can identify patterns, correlate events, and assess the severity of each alert more effectively.

The SOAR tool brings automation to the table, enabling analysts to handle alerts with greater efficiency. We automate routine tasks such as gathering additional information about the alerts, cross-referencing them with known indicators of compromise, and executing predefined response actions. This automation streamlines the triage and analysis process, freeing up valuable time for analysts to focus on more complex tasks that require their expertise.

By leveraging the enrichment from the MISP platform and the automation provided by the SOAR tool, our analysts can validate and triage the alerts in a more efficient manner. They can quickly identify false positives, prioritise the most critical alerts, and allocate resources effectively.

1.1.7 Use Case Development, Rule Creation and System Optimisation

Continuous use case development, rule development, and SIEM tuning are vital processes that ensure our solution remains up to date and maintains its ability to detect and respond to the latest threats. Cyberfort's approach to use case development involves the ongoing refinement and creation of specific scenarios that help identify potentially malicious activities or patterns within networks or systems. These use cases are developed based on an organisation's unique environment, threat landscape, and security requirements. By continuously developing new use cases, we can stay ahead of emerging threats and adapt our detection strategies accordingly.

Rule development is a vital step for us in maintaining an effective security solution. Generic rules are designed with a specific set of instructions or criteria that define how the SIEM should interpret and respond to incoming security events. These rules are based on known attack patterns or indicators of compromise. Cyberfort continuously develop and fine-tune these rules to ensure that the SIEM effectively identifies and alerts on relevant security incidents, reducing false positives and enhancing our overall accuracy of threat detection.

Our engineering team regularly tune the SIEM to optimise the system's configuration to achieve the best possible performance and effectiveness, we fine-tune various parameters such as log collection, data normalisation, correlation rules, and alerting thresholds.

By engaging in continuous use case development, rule development, and SIEM tuning, our solution remains proactive in its approach to cybersecurity. It is always looking for the latest threats and adapting its detection mechanisms to identify them. This ensures that our organisation stays ahead of potential security risks, minimises the impact of attacks, and maintains a robust security posture.

INPUT	VALIDATE	BUILD & TEST	ON-BOARD & OPERATIONALISE
• Adversary trends and behaviours • Targeted threat intelligence • Cyber Security incidents • Audit findings and gap analysis • Threat sharing communities. • Data sources and applications	Justify the need based on: • Business requirements • Regulatory compliance • IT environment changes • Cyber threat landscape • New applications	• Design • Build • Pilot	• On boarding • Roll-out • Monitoring

1.1.8 Data backup and restore, business continuity and DR

Cyberfort's MXDR service leverages multiple monitoring environments according to client need, cost and value.

All service components (including SOAR and TI) are implemented in a highly available, resilient architecture and are regularly backed up with restores tested as part of our ISO:27001 accredited business continuity and disaster recovery process.

Our ITSM runs within Atlassian Jira cloud within the UK region, and the configurations and data are regularly backed up with restores tested as part of our ISO:27001 accredited business continuity and disaster recovery process.

Where the service runs in Elastic SIEM, all components are deployed within the AWS region of your choice in a highly available and resilient manner with the configurations and data backed up regularly with restores tested as part of our ISO:27001 accredited business continuity and disaster recovery process.

Where the service leverages Microsoft Sentinel, this runs entirely within the client's Microsoft Azure tenant, meaning that your organisational policies and procedures relating to backup and restore will apply to the service data.

1.1.9 Evidencing Performance, Availability and value

SLA's and KPI's

Cyberfort ensure client satisfaction and service performance through a mix of SLA's and KPI's to ensure that the service is both aligned to client 's expectations and providing continuing evidence of improvement.

Fig.1: Demonstration of difference between SLA & KPI

The formal SLAs are constant throughout the service, the follow up KPI's are built together with each client to create meaningful indicators of performance, drive improvement, and evidence that the improvements are continuous and mapped to change within client 's environment, and that key data and systems are defended and available.

While SLAs are typically response and triage focussed, KPI examples include Mean-Time-To-Close, % detections from Cyberfort intel, hours saved through automation, detection alignment to MITRE, #times CIRT have been engaged and many more, and are trended over time to track improvements. However, critically these are built collaboratively with client to identify real time indicators, defensive actions, trends over time and baselines to iterative improvements.

The Technical Account Manager (TAM) owns the overall process, and Cyberfort actively manage and report on SLA's and KPI's. We monitor these in a variety of different ways including SIEM dashboards and monthly reports around evidence points and frequencies that we will define together with client. In all cases, the trend to iterative improvement is committed, and the early, during and late indicators are transparently monitored and regularly reported and discussed with client. The TAM will combine these outcomes and has a responsibility for correlating all KPI's and SLAs to drive and evidence performance and improvement transparently.

Cyberfort SLA Priority Levels - Incident Severity Matrix

A combination of incident urgency and impact allow Cyberfort to assign the relevant priority to the incident in line with the below matrixes:

Table 1: Priority Level Descriptions

P1 - Critical	**Critical: Active Cyber Attack** e.g. Evidence of an attacker operating from an escalation account (i.e. admin), malware or attack behaviour on a high-value host (i.e. Domain Controller), multiple machines displaying attach behaviour, data exfiltration.

P2 - High	**High: Immediate Operational Impact** e.g. Successful unauthorised logins, manual malicious commands being run on a host, alerts signifying an active persistent threat, multiple machines displaying similar attack evidence.
P3 - Medium	**Medium: Strong Likelihood of Operational Impact** e.g. Credential Loss due to phishing, verified malware execution on one or more hosts, detection of unauthorised program tasks or user activities.
P4 - Low	**Low: Moderate Possibility of Operational Impact** e.g. Malware quarantined or blocked, suspicious email(s) quarantined, suspicious inbound/outbound connections blocked, evidence of suspicious sign-in attempts/failures.
Informational	**Informational: Slight Possibility of Operational Impact / RFI** e.g. Vulnerability scan or risk assessment of environment reveals vulnerable services, security holes or other cyber risks or a request for information.

Table 2: Service Level Target Response Time

Priority	Initial Triage	Respond Within (SLA)	Validated Response (SLT)
Priority 1	30 minutes	1 working hour	1 working hour
Priority 2	30 minutes	2 working hour	4 working hours
Priority 3	30 minutes	8 working hour	8 working hours
Priority 4	30 minutes	Monthly report	Monthly report

1.1.10 Technical Requirements

Technical requirements are defined during onboarding and include:

- Ability to forward/collect appropriate logs to the designated cloud platform.
- A supported EDR tool (including Defender for Endpoint, Elastic Defender, Crowdstrike and others).
- A supported Identity tool (including Entra, Octa, and others).

1.1.11 Outage and Maintenance Management

The platforms that underpin our MXDR service are updated and supported at a platform level by:

- Elastic SIEM is supported by Elastic and AWS at an infrastructure level.
- Microsoft Sentinel is supported by Microsoft at an infrastructure and platform level.

Cyberfort monitors and manages the service on top of these components, providing service, outage, maintenance and change management of all components within the service, and monitors both Elastic and Microsoft Sentinel environments to alert on and address performance and availability issues.

1.1.12 Hosting Options and Locations

Both Elastic SIEM and Microsoft Sentinel can be hosted in any region of AWS (Elastic) and Azure (Sentinel) selected by the client. Our clients normally select the UK regions but can choose others for subsidiaries or for any other organisational reason.

The SOC, all of our resources and systems in use are hosted within the UK.

1.1.13 Access to Data (Upon Exit)

All service data remains the property of the client and is available to the client on exit.

In the case of Elastic SIEM, this data can be transferred to an Elastic SIEM instance owned by the client, or exported in multiple data formats, or deleted – as per the agreement with the client during the offboarding project.

In the case of Microsoft Sentinel, all service data is located within the clients Azure tenant and therefore access is retained upon exit.

Jira (ITSM) can be exported and supplied to the client or deleted as per the agreement with the client during the offboarding project.

1.1.14 Security

Cyberfort's MXDR service is governed by our stringent security policies, procedures and controls, which are all independently audited as part of our ISO27001 accreditation. The security controls include:

- All access to systems is operated on a least privilege basis, with escalation to privileged accounts granted on need and for a predetermined and authorised duration with other approved party approval.
- All systems are vulnerability managed and patched to restrict the attack surface.
- All systems comply with strict security baselines, with non-compliant systems prevented from access.
- All identities are protected by modern authentication, with MFA and granular conditional access.
- All code (including standard functions and configurations) is penetration tested and code reviewed throughout its lifecycle, with both manual and automated testing and validation.
- All data is encrypted in transit and at rest.
- All endpoints have an EDR tool that is monitored and has active responses.
- All services are pervasively monitored by our MXDR service, with 24x7x365 detections, analytics and responses delivering a full incident profile of appropriate events.
- Actionable threat intelligence is used for detection engineering, threat hunting and awareness (including actor tracking and TTPs).
- All users are regularly trained and tested on user awareness.

2. Onboarding and Offboarding Support

2.1 Deployment and phasing

To simplify the Cyberfort managed service deployment, we have developed a highly automated and programmatic approach to ensure rapid delivery, and a consistent and error-free method of onboarding clients.

Our managed service is deployed with dedicated engineering and analyst support delivering the following advantages for client.

- A reduction in the time required to onboard new clients, leading to cost savings.
- A reduction in costs and time investment from our clients to work with us on deployment.
- A flexible approach to deployment, adopting your regulatory and governance requirements and enforcing them through controls such as RBAC. This ensures the highest levels of security and lowest levels of access to our analysts.
- A structured approach to complex, multi-phased on-boarding, ensuring critical assets are delivered according to your risk profile and business needs.

The implementation of the service flows from Design to Deployment and then into an Operational phase

As part of the on-boarding process our project management team will work closely with you and will schedule a series of workshops during which the key technical and organisational information will be identified and validated leading to the production of a detailed project plan.

The project plan will include:

- Detailed steps and responsibilities
- Delivery method
- Resource requirements from both organisations
- Expected output
- Timelines for each step

Subject to the underlying architecture of your company, our rapid onboarding could mean value is seen within 20 minutes of the initial environment configuration.

The on-boarding process commences with a series of workshops in the early weeks of the process with different stakeholders to define the project in its different parameters, phases, and services. This is an in-depth process that will define on-boarding for the following weeks, and will cater for the scheduling, and the sequencing of the services.

The key aims are to ensure that the requisite technical knowledge is shared both ways, and the tasks understood before they are finalised in a work-plan between both parties. This will aim to cater for client priorities, and resource availability to perform parallel tasks which will be outlined for each service line.

- The workshops are accompanied by presentation and documentation that will aid the final definition of the process and will allow you to plan accordingly, factoring in your internal considerations.
- On boarding will be structured by mutual agreement, and workshops can be repeated or replicated for different lines of service or component which may have their own pre-requisites or planning associated.

- We will aim to gather as much information as early as possible in the process to allow our staff to perform as much of the implementation as possible without excessive needs to call on you for support or clarification.
- Once devices and log sources are connected, and the log collection has been verified and validated, we will enable the detection logic and analytics and then tune accordingly.
- Over a period of usually 3 months the telemetry and subsequent detection profile will be optimised against the MITRE ATT&CK framework to ensure most value is achieved from the available devices.
- During the on-boarding process consultants engage in a workshop setting to explain and review the service in full including the procedure for bespoke SIEM rule creation and bespoke use case creation if they are outside the MITRE ATT&CK framework. Relevant documentation about monitoring, triage and escalation is then generated and the outputs shared with clients.
- During on-boarding, fine-tuning is performed and continues during an initial period of service maturity development. The on-boarding process provides ample opportunity for you to discuss progress and process with technical service delivery leads.
- As part of our standard engagement process, we work with the business integration of our solution and how that would interact with you, including the creation of workflow management (incident escalation and management).

Offboarding plans are built consultatively with the client, and follow a similar approach, with the option of transferring the Elastic SIEM to a client owned environment or deleting the data.

2.2 Service constraints and customisation

We work together with clients on service design, leveraging individually or in combination Elastic SIEM, and Microsoft Sentinel. The design process is risk based and enables savings to be made through ingesting and automating log sources via the most appropriate, effective and efficient route – this continues throughout the life of the service.

We scope to risk and recommend effective combinations of logs, network, endpoint, identity and data-based ingestion to enable appropriate levels of visibility, detection and response.

The only major constraint of the service is we do not provide an on-premises service.

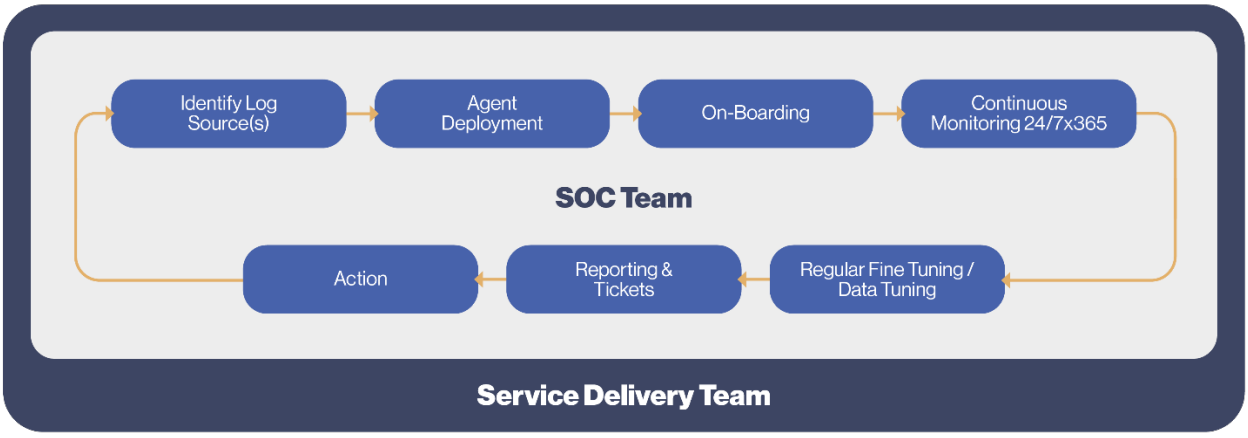
3. Service Management Approach

3.1 Service Delivery Teams

Cyberfort have assembled a cross-discipline team of Subject Matter Experts to provide a robust and comprehensive MXDR service to client.

- **Principal SOC Analyst:** Overseeing the day-to-day operational activities of the analysts and being an escalation point within the team.
- **Senior SOC Analysts:** third line escalation support, incident response, triage, malware analysis, system analysis and remediation advice.
- **SOC Analysts:** first line and 2nd line triage and investigation, incident response, system analysis and remediation advice.
- **Security Architect:** System design, reliability, innovation, and enhancement.
- **Senior Security Engineer:** Responsible for system configuration and maintenance.
- **Technical Account Manager:** client representative within Cyberfort.

Fig.2: Scope of the 24/7 MXDR Service



SOC Operations and SIEM Team

- Responsible for monitoring and detection resources
  - Assets they are protecting.
  - Assets used to provide the monitoring capability.
- Continuous Proactive Monitoring.
- Alert Ranking and Management.
- Threat Response
  - Playbook design, development, and release.
- Use Case and Rule Development and Management

  - Runbook development and release.
- Providing remediation advice and guidance.
- Log Management.
- client Reporting.
- Option to deploy Elastic Security EDR

SIEM Management and Monitoring

- 24/7/365 monitoring.
- Use case and rule development and optimisation.
- Data enrichment and automation.

Technical account management

- Dedicated Technical account manager - client Service Champion.
- Service metrics to complement technical reporting.
- MI Reporting and Analytics - Monthly Service reports and Quarterly Service Reviews
- Service Optimisation based on security events.
- Continuous Service Improvement – identifying opportunities for improvement.

Incident Response

- 24/7/365 Service Desk, resilient multi-site operation.
- Service Desk support for Technical Incident Responders.
- Incident reporting and management of in-flight communications.
- Wait time Management, Call outs and escalations.

Scheduling and Communications

- Forward maintenance schedule.
- Admin Support for Follow Up Actions and Escalations.
- Scheduled scenario-based service testing.
- Delivery Management support for Project Managers

4. Commercials & Pricing

4.1 Ordering & Invoicing Process

Please contact us for a quote via email at bidmanagement@cyberfortgroup.com

Orders are processed on receipt of a purchase order.

Prior to commencement of any work ordered via the G-Cloud framework, Cyberfort requires client acceptance of the order and also completion of a Call-Off Contract.

Clients are invoiced on a monthly basis or according to agreed milestones.

4.2 Service pricing model

Cyberfort's Managed Extended Detection and Response (MXDR) service pricing consists of two components.

- An onboarding charge which covers the implementation, configuration and onboarding of Elastic SIEM, Microsoft Sentinel and appropriate log sources to enable the service (a one-off charge) This includes the time of the engineer, project manager, technical account manager, consultants or engineers required and is dependent on the size and complexity of the deployment.
- The ongoing service charge covers the usage of the Elastic SIEM where required, including ingest, analytics and storage. The monitoring, detection, response and incident handling activities in addition to content creation (including use cases, dashboards, automations, threat intelligence investigations) and technical account management including continuous improvement, reporting and support. In addition, this charge covers the usage of the Elastic SIEM where required, including ingest, analytics and storage.

Please refer to our Pricing document for more details.

4.3 Minimum contract period

Contract terms will be provided at the time of quotation, based on specification. These will not exceed the maximum contract constraints of the G-Cloud framework.

5. Governance Compliance

Cyberfort confirm that we will deliver our services to clients in line with all industry and Government recognised standards, best practice and legal regulations, including but not limited to the following:

5.1 GDPR

We adhere to the legal and statutory requirements outlined in the UK Data Protection Act 2018 and the General Data Protection Regulations (GDPR). Our organisation has a current registered Information Commissioners Office (ICO) certificate for Data Protection.

5.2 Government and industry standards

Throughout the life of any contract, our consultants will ensure that all service standard principles are adhered to so that clients can be assured that all delivered outcomes conform with Government and industry standards and expectations. Our teams are deeply experienced in operating services, to deliver outcomes and outputs that fully comply with:

- The principles defined in the Government's Service Standard and Technology Code of Practice (TCoP).
- The Government Functional Standard (GovS 007: Security), ensuring that the stated principles (for example security objectives are aligned to government policy and organisational objectives) are applied to all projects.
- Open standards supported include TOGAF, NIST-CSF, ISO/IEC27000, SANS and OWASP.
- Regulation frameworks including, Cyber Security and Resilience Bill, Digital Operational Resilience Act (DORA), and NIS2 Directive.
- Government Cyber Security Strategy, including National Cyber Security Centre (NCSC).
- As an NCSC assured Cyber Security Consultancy, we are members of the NCSC Assured Consultancy Scheme Community Network and leverage the CiSP (Cyber Information Sharing) platform.

5.3 Quality Management

Further, we have a fully implemented Quality Management System (QMS) and are certified to ISO 9001:2015 International Standard, which details our policy, objectives and processes, as well as demonstrating how our QMS framework enhances client satisfaction whilst ensuring consistent delivery of product and services is maintained to meet client, statutory and regulatory requirements.

Our delivery is underpinned by certifications and associated management systems including:

- ISO:27001
- ISO:14001
- ISO:9001
- ISO:45001
- Cyber Essentials Plus
- CREST Certified Body CE
- CREST Penetration testing
- NHS Digital Toolbox
- PCI DSS
- DSPT
- NCSC Cyber Security Consultancy
- NCSC CHECK ITHC

About Cyberfort

Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

Cyberfort

Care about the impacts we make on the Environment, Social and Governance.

We are passionate about empowering our employees, suppliers, customers, and the cyber security ecosystem to create a better world for our business and the communities we participate in, for example:

As a member of Neurodiversity in Business (NiB) and Disability Confident Employer

Cyberfort are supporting those with physical and neurodiverse disabilities, by disarming barriers for people with disabilities and ensuring equal opportunities for all.

Cyberfort are inspiring and attracting young people to the world of cybersecurity.

We support the development of their passion for technology through Apprenticeships, Graduate Schemes, CyberFirst and school education/awareness.

We are committed to achieving net zero carbon emissions by 2050.

Cyberfort have clear plans and activities that deliver environmental benefits by increasing the energy efficiency of our operations, reduce our waste, and protect our communities.

Our Values

Teamwork | Curiosity

Ownership | Agile | Innovative

Cyberfort

Accreditations

We are proud of the extensive list of industry and government accreditations we hold. We understand the need for independent validation when entrusting the security of valuable or sensitive data to a third party.

Our Vision

To be an integral part of the cyber security ecosystem, providing assured, highly skilled and reliable security services to businesses and government departments. Embodying the UK Cyber Security Strategy, through trusted partnerships we aim to empower businesses and government departments with confidence, making the world a safe and secure place to conduct business.

Our Mission

To provide our customers with an agile and innovative approach to help them overcome their cyber security challenges. Through a collaborative approach with our customers we design, build and operate their cyber security environments resulting in a secure and resilient infrastructure, providing a safe environment for employees, service users and stakeholders to conduct their business in the knowledge that their critical data remains safe in an ever-changing digital world.

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com